ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Fog Computing a Paradigm: Scenarios And Security Issues

[1] Sai Keerthi.Tulluru, [2] Dr.Anuradha S.G
[1] Dept of Computer Science, RYMEC, Ballari, India
[2] Associate Professor, Dept of Computer Science RYMEC Ballari, India

Abstract: **- Fog computing is a paradigm that extends cloud computing and services to the edge of the network. Fog computing provides data, storage, and application services to end users. In Fog computing user data is outsourced and user's control over dated is handed over to fog node, which introduces same security threats as it is in cloud computing. Fog computing is well suited for real time analytics and big data .Security incidents regarding fog computing are posed by the hostile attack and main-in-the-middle attacks.**

Keywords**: Fog computing, Security issues, IOT and Cloud computing, MD5.**

I. INTRODUCTION

Fog computing is developed as a technology to bridge gap between remote data centers and IoT devices. Fog devices face any security and privacy threats. The security and privacy should be addressed in every layer in fog computing. The authentication is an important issue for security of fog computing since services are provided to massive-scale end users. The concept of fog computing involves communication among a number of IoT devices, fog nodes, and back-end clouds the communication should be secure. However, due to salient feature of fog computing, existing solutions for secure communications cannot be applied directly. If wrong information is spread malicious user can cause big problems and leads to a lot of damage. Virtualization technology is basically and prevented from access of other operating systems, but if there is a problem in kernel mode, it does not prevent. In fog computing environment, much of information is stored in fog node and if wrong information is spread by exploiting vulnerability, we expect that it is in a big problem. In fog computing environment, fog nodes provide service based on the information collected from the IoT node. When some IoT nodes provide wrong information, it can affect people. Attackers have a chance to compromise various devices with sensors.

II. RELATED WORK

[1] On security and privacy issues of fog computing supported Iot environment, author Kanghyo discussed the need to configure the secure fog computing environment through security technologies.
[2] Fog computing for the internet of things: security and privacy issues, author Arwa Alwaris investigated and discussed security and privacy challenges of introducing fog computing in Iot environments.
[3]The fog computing paradigm: scenarios and security issues, author sheng wen focused on fog computing advantages for services in several domains and provide the analysis of the state-of-the-art and security issues in current paradigm.
[4]Fog computing issues and challenges in security forensics, author Yifan Wang mentioned fog computing: as a security technology has been used to secure cloud via combining decoy technology with other technologies.
[5] Fog and Iot: An overview of research opportunities, author Mung Chaing about how fog is starting to replace the future landscape of multiple industries
[6]Fog computing to protect real and sensitivity information in cloud, author Ashwini and Mrs. Anuradha said fog computing is a paradigm which helps the behavior of the user and providing security to the user data.
[7] Security and privacy Issues of Fog Computing: A Survey, author Shanhe Yi discussed several security and privacy issues in context of fog computing.
Organization of Paper: Section III contains the security issues in fog computing, Section IV describes the need for the fog, Section V describes where do we need fog, Section VI describes how to secure cloud computing using fog computing, Section VII is conclusion and Section VIII is References.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

III. SECURITY ISSUES IN FOG COMPUTING

Man-in-the-middle attack: It is a type of attack that occurs when malicious user insert himself into communication between people or system.

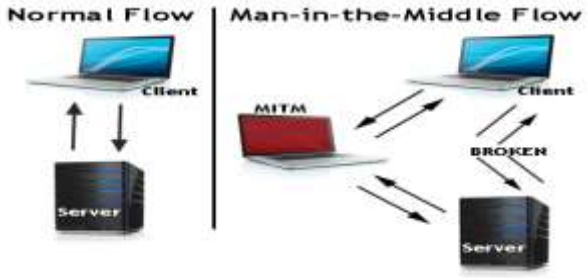

Figure 1: Man-in-the-middle attack

Other forms of session hijacking:
Sidejacking: Side jacking attack involves sniffing data packets to steal session cookies and hijack a user's session.
Evil Twin: Evil Twin is a rouge network that seems to be actual network but it's not. If unknowingly user joins this network, the attacker can launch a man-in-the-middle attack, intercepting all data between you and the network.
Sniffing: Sniffing involves a malicious actor using readily available software to intercept data being sent from, or to, your device.

Intrusion detection:

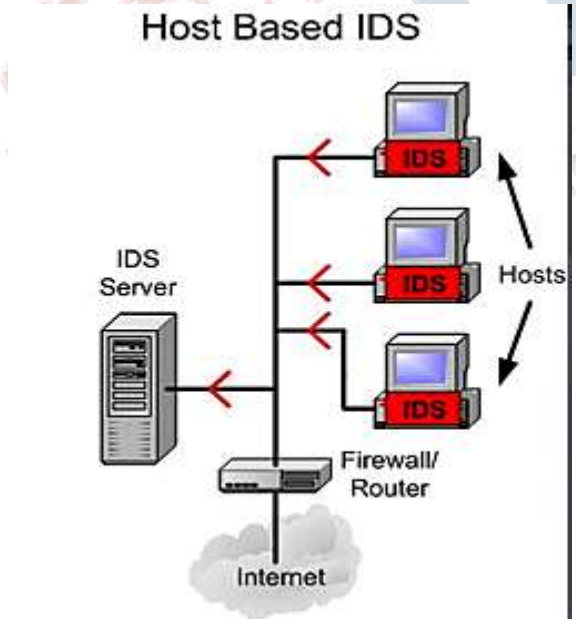

Figure 2: Intrusion Detection System

This system analyses and monitors
access control policy
A log file
User log information to detect intrusion behavior.
Intrusion detection techniques are widely deployed in cloud system to mitigate attacks such as:
Insider attack
Flooding attack
Port Scanning
Attacks on virtual machines and hypervisor.
It can be run on network side in order to detect malicious activities such as Port scanning, DoS.

C) Malicious Detection Technique in Fog Computing Environments: When fog nodes are compromised, hybrid detection technique is useful to detect malicious code in fog nodes. It is combined with signature-Based Detection technique and Behavior Based Detection technique.

D)Malicious Fog Node Problem: In order to afford service to user, fog nodes process data received from the Iot devices. If workload is heavy it is divided and processed by several fog nodes. If some fog nodes are compounded by malicious user it is difficult to ensure the wholeness of data. So, before computation begins, fog nodes must trust each other for which authentication protocol is needed.

E) Data Protection: The exponential volume of data generated Iot devices is increasing and this data should be preserved not only at communication level but also at processing level. This data is usually sent for fog nodes for processing. At this point the integrity of data should be analyzed without exposing it. Because of limited resources, it is difficult to encrypt or decrypt data on IoT devices.
F) Data Management Issues: Fog nodes are geographically distributed, making it difficult to know data's location. The user wants to be provides with the same services in other area and it is difficult for user to know whether the node provides the same service. Some nodes by having duplicate files may waste resource.

IV. WHY DO WE NEED FOG?

Fog computing is not replacement of cloud computing. As Fog computing is implemented at edge of network, it provides edge location, location awareness, low latency, support for mobility and quality-of-services (QoS) for streaming and real applications. The Fog computing paradigm is well positioned for real time big data analytic, support densely distributed data collection points, and provides advantages in entertainment, personal computing and other applications.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

V. WHAT CAN WE DO WITH FOG?

On the role of Fog computing in the following scenarios. The advantages of Fog computing satisfies the requirements of applications in these scenarios:

Smart Grid: Energy load balancing applications may run on the network edge devices, such as micro-grids and smart meter. Based on demand for energy, availability and the lowest price, these devices automatically switch to alternative energies like solar and wind.

Figure3 : Fog computing in smart grid

Smart Traffic lights and connected vehicles: Video camera that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic. Smart street lights interact locally with sensors and detect presence of pedestrian and bikers, and measure the distance and speed of approaching vehicles.

Wireless sensor and Actuator Networks: Traditional wireless sensor networks fall short in applications that go beyond sensing and tracking, but require actuators to exert physical actions like opening, closing or even carrying sensors. In this, actuators serving as fog nodes can control the measurement process itself, the stability and the oscillatory behaviors' by creating a closed-loop system.

Decentralized Smart building control: The applications of this scenario are facilitated by wireless sensors deployed to measure temperature, humidity, or levels of various gases in the building atmosphere. In this case, information can be exchanged among all sensors in a floor, and their readings can be combined to form reliable measurements. Sensors will use distributed decision making and activation at fog devices to react to data. The system components may then work together to lower the temperature inject fresh air or open windows.

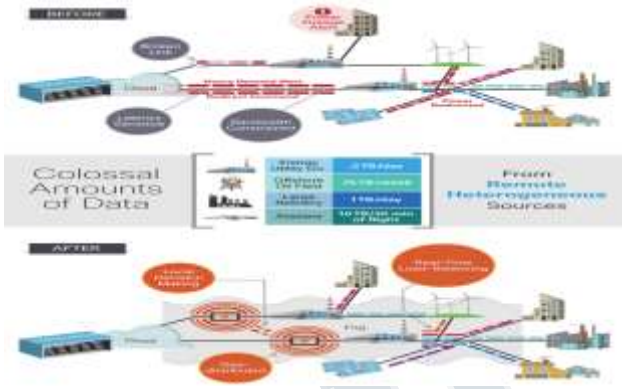

Figure 4: Represents the grids connected before and after Fog

VI. SECURING CLOUD COMPUTING USING FOG COMPUTING

One approach using decoy technology and user Behavior Profiling

i) Decoy System: Decoy data, such as decoy documents ,honeypots and other bogus information which can be used for detecting abnormal access to information that can be generated on demand and to 'poison' the ex-filtrated information.

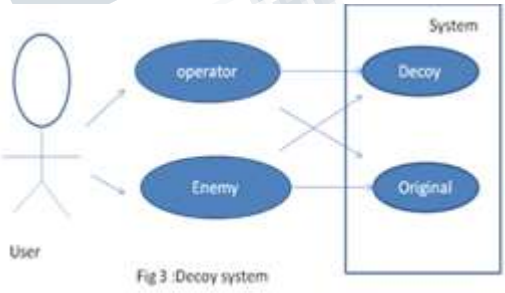

Fig 3 :Decoy system

The decoy will puzzle an attacker into believing they have ex-filtrated valuable information, but they have actually not. When the unauthorized access to cloud is noticed, decoy information is returned by the cloud and delivered in such way it appears to be normal. This is technology may be combined with user behavior profiling technology to secure user's information in cloud.

ii.User Behavior Profiling: It is expected that access to a user's information in cloud will exhibit a casual means of access. User profiling is familiar technology that can be applied to model in what way, how much, when user access an information in cloud. Such 'normal user' can be continuously checked to determine whether abnormal access to a user's information is arising. This method is commonly used in fraud detection applications.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Combining User Behavior and Decoy Technology for Masquerade Attack: User Behavior Profiling: Legitimate users of a computer system are familiar with the files on that system and where they are placed. Any search for specific files would be targeted. A masquerade, however, which gets access to the victim's system illegitimately, is unfamiliar with structure and contents of the system. Their such for files would be widespread and untargeted. Based on these key assumptions, we profiled user search behavior and developed model with help of one class modeling technique, namely one class provision vector machine. The purpose of one class modeling is it ability of building classifier without sharing data from other users. The privacy of the user and their data is preserved.

Decoy Technology: We placed traps within the file system. The traps are decoy files downloaded from fog computing site, an automated service that offers several types of decoy documents such as tax return forms, medical records credit.

The advantages of placing decoys in a file system are:

1) The detection of masquerade activity.

2) The confusing the attacker and the additional costs incurred to distinguish real and bogus information, and

3) The deterrence effect which, although hard to measure, plays a significant role in preventing masquerade activity by risk-averse attackers.

Combining the Two Techniques: The correlation of behavior anomaly detection with trap-based decoy files should provide stronger evidence of misconduct, and therefore improve a detector's accuracy. We hypothesis that detecting abnormal search operations performed prior to an unsuspecting user opening a decoy file will strengthen the suspicion that the user is indeed impersonating another victim user.

This Scenario covers the threat model of illegitimate access to cloud data. Furthermore, an accidental opening of a decoy file by a legitimate user might be recognized as an accident if the search behavior is not deemed abnormal. In other words, detecting abnormal search and decoy files together may make a very effective masquerade detection system.

To overcome these techniques fog computing provides solution that results of our experiments suggest that user profile are accurate enough to detect unauthorized cloud access.

B. Other approach is cryptographic hash function

A cryptographic hash function is a hash function which takes input (or message) and returns a fixed-size alphanumeric string. The string is called message digest. Hash functions are routinely used t check integrity or for error detection of transmitted messages. A Hash function which will be used for cryptographic purposes should have some properties:

A cryptographic hash function should be one-way. Knowing an output h of the hash function it should computationally infeasible to find a message m which hashes to that output; i.e., for which h(m)=h

A cryptographic hash function should be second pre-image resistant –a given message m1,it should be computationally infeasible to find another message m2 with m m 1 2!=having h h(m m 1 2)=()

A cryptographic hash function should be strongly collision free. It should be computationally infeasible to find two different inputs that have the same hash; i.e., it should be computationally infeasible to find messages m m 1 2!=having h h(m m 1 2)=()

Of course, the number of inputs is much larger than the number of outputs, so collisions will occur but collisions should be unlikely.

The popular used hash functions-MD(message digest),SHA(secure hash algorithm).

The MD family compromises of hash functions MD2,MD4, MD5 and MD6-bit hash functions. The MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file.

MD5 algorithm

MD5 algorithm can be used as a digital signature mechanism.

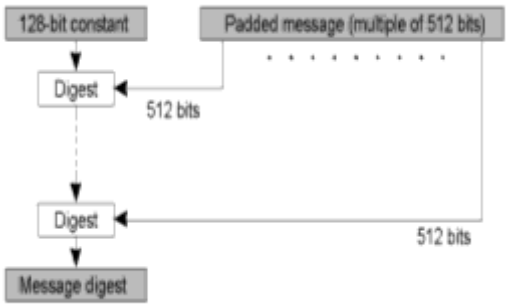

Figure 6:MD5 algorithm structure

MD5 takes as input a message of arbitrary length and produces a 128 bit "fingerprint" or "message" of the input. Intended where a large file must be compressed in secure manner before being encrypted with a private key under a public-key cryptosystem such as PGP.

Suppose a b-bit message as input, and that we need to find its message digest.

Steps in MD5 algorithm

STEP1: Append padded bits .

The input message is padded so that its length is congruent to 448, modulo 512.Means extended to just 64 bits shy of being of 512 bits long. A single "1" bit is

appended to the message, and then "0" bits are appended so that the length in bits equals 448 modulo 512.
STEP2: appended length
A 64 bit representation of b is appended to the result of the previous step. The resulting message has a length that is an exact multiple of 512 bits.
STEP3: initialize MD buffer
A four-word buffer (A, B , C, D) is used to compute the message digest. Here each of A, B, C, D is a 32 bit register. These registers are initialized to the following values in hexadecimal:
Word A: 01 23 45 67
Word B: 89 ab cd ef
Word C: fe dc ba 98
Word D: 76 54 32 10
STEP 4:Process message in 16-word blocks
Four auxiliary functions that takes as input three 32-bit words and produce as output one 32-bit word.
F(X,Y,Z)= XY v not(X)Z
G(Y,Y, Z)=XZ v Y not(Z)
H(X, Y, Z)=X xor Y xor Z
I(X, Y, Z)=Y xor(X v not(Z)
If the bits of X,Y,Z are independent and unbiased, the each bit of F(X,Y,Z), G(X,Y,Z), H(X,Y,Z) and I(X,Y,Z) will be independent and unbiased.
STEP 5:
The message digest produced as output is A,B,C,D, i.e., output begins with the low-order bits of A and end with the high-order byte of D.

VII. CONCLUSION

Data theft attack became serious issue for cloud service providers. Fog computing is a paradigm which helps in monitoring the behavior of the user and providing security to user data. In fog computing we present a new approach for solving the problems of insider data theft attacks in a cloud using dynamically generated decoy files .So by using decoy technology with user behavior profiling we can minimize insider attack in cloud. Cryptographic hash functions are useful tool in protection of integrity.MD5 algorithm secures a large file and is easy to implement and simple. The difficult is when two messages are of same message digest.

REFERENCES

[1] Lee, Kanghyo, et al. "On security and privacy issues of fog computing supported Internet of Things environment." Network of the Future (NOF), 2015 6th International Conference on the. IEEE, 2015.

[2] Alrawais, Arwa, et al. "Fog Computing for the Internet of Things: Security and Privacy Issues." IEEE Internet Computing 21.2 (2017): 34-42.

[3] Stojmenovic, Ivan, and Sheng Wen. "The fog computing paradigm: Scenarios and security issues." Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. IEEE, 2014.

[4] Wang, Yifan, Tetsutaro Uehara, and Ryoichi Sasaki. "Fog computing: issues and challenges in security and forensics." Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual. Vol. 3, IEEE, 2015

[5] Chiang, Mung, and Tao Zhang. "Fog and IoT: An overview of research opportunities." IEEE Internet of Things Journal 3.6 (2016): 854-864.

[6] Ashwini, Thogaricheti, and Mrs. Anuradha SG. "Fog Computing to protect real and sensitivity information in Cloud."

[7] Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." International Conference on Wireless Algorithms, Systems, and Applications. Springer International Publishing, 2015.